PAUL HASTINGS

Stay Current

April 2024

Follow @Paul_Hastings

# *CISA Proposes Sweeping Cybersecurity Incident Reporting for U.S. Companies*

By John Gasparini, Aaron Charfoos, Kimia Favagehi, Hannah Edmonds & Marisa Polowitz

On March 27, 2024, the Cybersecurity & Infrastructure Security Agency ("CISA") released proposed regulations requiring expansive new cybersecurity incident and ransomware payment reporting across sixteen "critical infrastructure sectors" spanning broad swaths of the U.S. economy, from financial services to information technology, transportation, and energy and water utilities, among others. Unlike many other U.S. cyber incident reporting requirements (which have reporting timelines stretching weeks or months, triggered primarily by personal data breaches), these rules will require reporting of a broad array of "substantial cybersecurity incidents" within 72 hours and ransomware payments within 24 hours.

While the draft regulations remain subject to public comment, key provisions are prescribed by statute and are unlikely to change before finalization. CISA must finalize these regulations within 18 months of publication (but is not obligated to use all that time), so companies should promptly consider impacts and begin planning for compliance in the near term. Specifically, any entity potentially subject to these regulations should promptly:

1. Evaluate whether they will be subject to these regulations. For some entities this will be an easy analysis but, for many, this could be a complicated analysis, as the criteria are varied and extremely detailed;

2. Consider participating (either directly, or through trade associations) in the public comment period which will start on April 4th and last for 60 days; and

3. Assess the need for updates and expansion of incident response plans and procedures in anticipation of these reporting requirements. While the rules may not be finalized for up to 18 months, for many entities, it will take substantial time and effort to prepare.

## Background

CISA's Notice of Proposed Rulemaking ("NPRM") implements key incident reporting requirements of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"). CIRCIA requires CISA to adopt regulations requiring "covered entities" across sixteen critical infrastructure sectors to report certain "substantial" cyber incidents within 72 hours, and report ransomware payments within 24 hours. While CISA has latitude to interpret these requirements (and the 477-page NPRM reflects detailed analysis of the criteria for inclusion in each of the 16 sectors, as well as feedback from an array of public engagement steps CISA took in preparing the regulations), the most challenging details—particularly

the timeline for reporting—are set in the statute and are unlikely to change (despite calls to align reporting more closely with other sectoral regulators' requirements or with the SEC's recently adopted material cyber incident disclosure rules).

## Entities Covered by the Reporting Rules

The CIRCIA reporting requirements apply only to "covered entities", and CISA goes to great lengths to spell out its proposed criteria for evaluating which entities the regulation should cover. In interpreting CIRCIA, CISA proposes two paths to applicability. First, it proposes size-based thresholds (tied to revenue and employee counts) across all sixteen sectors. Second, to ensure it captures all critical facilities, even where operated by smaller entities, the NPRM includes further specific criteria for thirteen sectors. If an entity meets either the size criteria or any of the sector-specific criteria, it will be a Covered Entity under CIRCIA.

### *Size-Based Criteria*

The NPRM ties the size-based criteria to the Small Business Administration's processes and guidance. In short, if an entity qualifies as a "small business" in its industry under the SBA's rules, then it should be exempt from these regulations unless it meets one of the sector-specific criteria.

### *Sectoral Criteria*

The sixteen critical infrastructure sectors are defined by Presidential Policy Directive 21, released in 2013. The NPRM discusses each of those in detail, prescribing specific criteria for thirteen of them, while for the other three (Commercial Facilities, Dams, and Food and Agriculture), CISA intends to rely on the size-based thresholds to appropriately capture relevant entities.

Those thirteen sectors (and key elements of their eligibility criteria) are:

1. **Chemical**. Limited to entities that own or operate a "covered chemical facility subject to the Chemical Facility Anti-Terrorism Standards".

2. **Communications**. Including any entity that provides communications services by wire or radio, as defined under the Communications Act. This includes an array of communications companies subject to varying degrees of Federal Communications Commission ("FCC") oversight (including those not required under FCC rules to report cyber events to that agency).

3. **Critical Manufacturing**. Encompassing any entity that owns or has business operations engaged in one or more of four categories of manufacturing: primary metal manufacturing; machinery manufacturing; electrical equipment, appliance, and component manufacturing; and transportation equipment manufacturing.

4. **Defense Industrial Base**. Covering any entity that is a contractor or subcontractor "required to report cyber incidents to DOD" pursuant to DFARS requirements.

5. **Emergency Services**. Extending to any entity that provides one or more of the following emergency services or functions to a population of 50,000 individuals: law enforcement; fire and rescue services; emergency medical services; emergency management; and public works that contribute to public health and safety.

6. **Energy**. Limited to any entity required to report cybersecurity incidents under NERC's CIP Reliability standards or required to file an Electric Emergency Incident and Disturbance Report with the Department of Energy.

7. **Financial Services**. Encompassing entities (i) required to report cyber incidents to their primary Federal regulator; (ii) whose primary regulator (e.g. the CFTC) has expressed an intention to require such reporting; or (iii) "encouraged or expected" to report incidents pursuant to an Advisory Bulletin (such as money services businesses).

8. **Government Facilities**. Capturing certain State, Local, Tribal, and Territorial government facilities, educational facilities, and elections-related entities.

9. **Healthcare and Public Health**. Extending to entities that (i) own or operate hospitals with 100 or more beds, or any critical access hospital; (ii) manufacturers of certain drugs; and (iii) manufacturers of Class II and Class III medical devices.

10. **Information Technology**. Primarily comprising (i) any entity that knowingly provides IT hardware, software, systems, or services to the Federal government; (ii) any entity that developed and continues to sell, license, or maintain any "critical software" as designated by NIST; (iii) any OEM, vendor, or integrator of Operational Technology ("OT") hardware and software; and (iv) any entity that performs functions related to domain name operations.

11. **Nuclear Reactors**, **Materials**, **and Waste**. Comprising any entity that owns or operates a commercial nuclear power reactor or fuel cycle facility.

12. **Transportation**. Transportation has numerous criteria intended to capture owners and operators of various non-maritime transportation system infrastructure such as freight railroad, public transportation and passenger railroad, pipelines, over-the-road bus, passenger and cargo aircraft, indirect air carriers, airports, and certified cargo screening facilities, as well as those who own or operate vessels, facilities, or outer continental shelf facilities under various Federal regulations.

13. **Water and Wastewater Systems**. Covering owners and operators of any community water system or publicly owned treatment works, in each case serving more than 3,300 people.

While many entities will clearly fall within (or outside) of these categories, for many, it will be a more complex analysis—companies should begin that consideration now as preparations for CIRCIA compliance could take time.

### Which Incidents are Reportable?

CIRCIA requires reporting only of "covered cyber incidents" which it proposes to define as those that are "substantial" and impact a covered entity. As with materiality in the SEC reporting context, the question of "substantiality" will be somewhat subjective and it will take time for best practices to emerge. CISA proposes, however, that a "substantial cyber incident" is one leading to any of the following outcomes:

1. A substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;

2. A serious impact on the safety and resiliency of a covered entity's operational systems and processes;

3. A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services; or

4. Unauthorized access to a covered entity's information system or network, or any nonpublic information … that is facilitated through or caused by either a compromise of a cloud service provider, managed service provider, other third-party data hosting provider, or a supply chain compromise.

This includes any incident with these impacts regardless of the cause—CISA notes in particular that a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; a supply chain compromise; a denial-of-service attack; a ransomware attack; or exploitation of a zero-day vulnerability, could all qualify as "substantial" and thus reportable incidents.

This subjective analysis (and the tight 72-hour timeline) poses a new challenge for many entities, particularly those with few or no existing cyber incident reporting requirements. As a result, companies may need to update incident response plans, conduct additional tabletop exercises, and plan their incident response activities more thoroughly to be able to quickly and effectively make these assessments.

There are three specific exceptions for types of incidents which do not need to be reported:

1. Any lawfully authorized activity of a U.S. Government entity or SLTT Government entity, including activities undertaken pursuant to a warrant or other judicial process;

2. Any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; or

3. The threat of disruption as extortion.

Lastly, there are a handful of circumstances outlined under which entities are exempt from the reporting requirements (e.g. where a Federal agency is covered by FISMA reporting obligations, for example); however, these are likely to apply (at least in the near term) in only extremely narrow circumstances to very limited sets of entities.

### Contents of Reports

The NPRM spells out an extensive and detailed list of information CISA expects covered entities to provide, whether in an initial report, a supplemental submission, or in response to a Request for Information ("RFI") from CISA themselves. The bulk of this information is required for reporting covered cyber incidents—reports of ransomware payments include similar requirements, in addition to detailed information about ransom payments.

Broadly speaking, CISA expects reports to cover the following key areas (and include details including, but not limited to, those listed with each section):

- **Identifying information** about the covered entity, including details of its critical infrastructure sector, trade and legal names, and other details;

- **Contact information** for the covered entity, and a third party if reporting on behalf of a covered entity;
- **Description of the incident**, including descriptions of impacted systems (including technical and physical locations of impacted systems); whether there was unauthorized access; date ranges, operational impacts, potential impacts; and the nature of information believed to have been accessed;
- **Vulnerabilities**, **Security Defenses**, **and Tactics**, **Techniques**, **and Procedures**, such as the specific vulnerabilities exploited; security controls in place (and which ones failed or were insufficient); type of incident, and tactics, techniques, and procedures used by threat actors, as well as indicators of compromise;
- **Perpetrator identity**, to the extent known;
- **Mitigation & Response Information**, including details of mitigation measures in place, responsive actions taken, the current status of the incident, and any engagement with law enforcement or other third parties for assistance; and

In addition, ransomware reports must include details of payments including amounts, dates, currency types, what demands were made vs payment actually rendered, and payment instructions, as well as the results of the payment having been made.

CISA acknowledges not all information will be available for initial reports, but expressly anticipates entities providing *all* of the required information either initially or through subsequent reports and has the ability to issue RFIs and even subpoenas to seek information it believes it is entitled to and which has not been provided.

### Timing

Initial reports are due to CISA within 72 hours of determining that an incident is reportable—that is, determining that it is "substantial" and therefore is a "covered incident". Ransomware reports are due within 24 hours of a payment being made.

Subsequent reports are required to be made "promptly", as information required and not previously provided is obtained by the covered entity, or where the investigation establishes that a previously submitted report is materially incorrect or incomplete. The NPRM does not set a specific timeline for supplemental reports (except to note that a supplemental report disclosing a ransomware payment is subject to the same 24-hour clock as a ransomware payment report), opting, instead, for a common-usage definition of "without delay or as soon as possible". Given the rapidly evolving nature of cyber investigations, this could result in significant burden in more complex investigations where many rounds of incremental reporting may be required; this may be a key area where commenters seek further refinements to the proposed rules before they are finalized.

### Privilege and Confidentiality

CISA recognized in response to public input that the contents of CIRCIA reports will be extremely sensitive for reporting entities. In addition to containing extensive technical details, CISA is seeking information that goes to the root cause of, and responsibility for, cybersecurity incidents—including seeking specific indications of failed internal controls, for example. Such information could easily be used by regulators or other litigants against companies and the NPRM extends some protections to this

information as a result. In general, the NPRM proposes to exclude the contents of reports from use in regulatory and enforcement actions; exclude such reports from discovery or other demands; treat such information as confidential and sensitive trade secrets, and expressly provide that sharing such information does not constitute a waiver of any privilege.

Of note, however, is that these protections only extend to the reports themselves and materials prepared for the "sole" purpose of preparing a CIRCIA report. The underlying facts would not be privileged and could be discovered through litigation anyway; similarly, if a regulatory or law enforcement agency had these facts through means other than a CIRCIA report, those facts could still be used in an enforcement action. Thus, companies will need to continue to think extremely carefully about the records created in the course of responding to cybersecurity incidents and preparing incident reports.

### Other Issues

CISA's NPRM, weighing in at nearly 500 pages, provides extensive detail about the interpretation of almost every aspect of these rules; enforcement when companies fail to report; record retention requirements; and other issues. Future Paul Hastings updates on our PH Privacy blog will take a deeper look at various aspects of the NPRM as follow-ups to this overview of key provisions.

### Next Steps

As an immediate matter, there are several next steps that any entity which *may* fit in one of the sixteen sectors should consider:

1. First and foremost, work with counsel to evaluate whether you are likely within the scope of these reporting requirements. For some entities this will be an easy analysis, but for many this could be a complicated analysis. For small but quickly growing companies, this is something to monitor on an ongoing basis, as well—while you may be exempt now, that may not be the case when the regulations ultimately take effect.

2. Entities likely to be covered should consider participating (either directly, or through trade associations) in the public comment period which will start on April 4th and last for at least 60 days.

3. Work with expert advisors to consider whether, and to what extent, your current incident response plans need to be updated or refined to account for these forthcoming requirements. While CISA has 18 months to finalize these rules, they are not required to use all that time, and unless Congress repeals CIRCIA, they are unlikely to simply abandon this effort entirely. It may take some entities (particularly those who have not previously had any cyber incident reporting obligations) substantial time to plan and prepare for increased cyber reporting and related scrutiny.

Paul Hastings attorneys, and consultants in our Privacy and Security Solutions Group, are closely monitoring CIRCIA developments and routinely assist clients with cyber incident preparedness, response, and reporting issues. Please contact any member of the Paul Hastings team with any questions or to discuss these issues further.

✧ ✧ ✧

*If you have any questions concerning these developing issues, please do not hesitate to contact either of the following Paul Hastings lawyers:*

**Chicago**

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

**Washington D.C.**

John Gasparini
1.202.551.1925
johngasparini@paulhastings.com